The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

04/29/2014

SUBJECT:

Vulnerability in Adobe Flash Player Could Allow Remote Code Execution (APSB14-13)

EXECUTIVE SUMMARY:

A vulnerability has been discovered in Adobe Flash Player. Adobe Flash Player is a widely distributed multimedia and application player used to enhance the user experience when visiting web pages or reading email messages. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

THREAT INTELLIGENCE:

This vulnerability is currently being exploited in the wild. Kaspersky Lab has reported that an active exploit for this vulnerability was discovered on a compromised website at hxxp://jpic[dot]gov[dot]sy.

SYSTEMS AFFECTED:

- Adobe Flash Player 13.0.0.182 and earlier versions for Windows
- Adobe Flash Player 13.0.0.201 and earlier versions for Macintosh
- Adobe Flash Player 11.2.202.350 and earlier versions for Linux

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

Adobe Flash Player is prone to a remote buffer overflow vulnerability. This vulnerability exists in the Pixel Bender component of Adobe Flash. The vulnerability may be exploited in a way that could allow an attacker to execute arbitrary code, in the context of the current user, within Adobe Flash. An attacker could host a website with a specially crafted Small Web Format (SWF) file designed to take advantage of this vulnerability, and then convince or trick an unsuspecting user to visit their site.

Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Remind users not to visit untrusted websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.

REFERENCES:

Adobe:

http://helpx.adobe.com/security/products/flash-player/apsb14-13.html

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0515

Securelist:

http://www.securelist.com/en/blog/8212/New_Flash_Player_0_day_CVE_2014_0515_used_in_watering_hole_attacks